PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00 — A1

(11) International Publication Number: **WO 00/16179**

(43) International Publication Date: 23 March 2000 (23.03.00)

(21) International Application Number: PCT/EE99/00001

(22) International Filing Date: 13 September 1999 (13.09.99)

(30) Priority Data:
P199800237 11 September 1998 (11.09.98) EE

(71)(72) Applicant and Inventor: MARANDI, Mart [EE/EE]; Tuule tee 7/2, EE12111 Tallinn (EE).

(74) Agents: KERNU, Urmas et al.; A.A.A. Baltic Service Company, P.O. Box 3926, EE10509 Tallinn (EE).

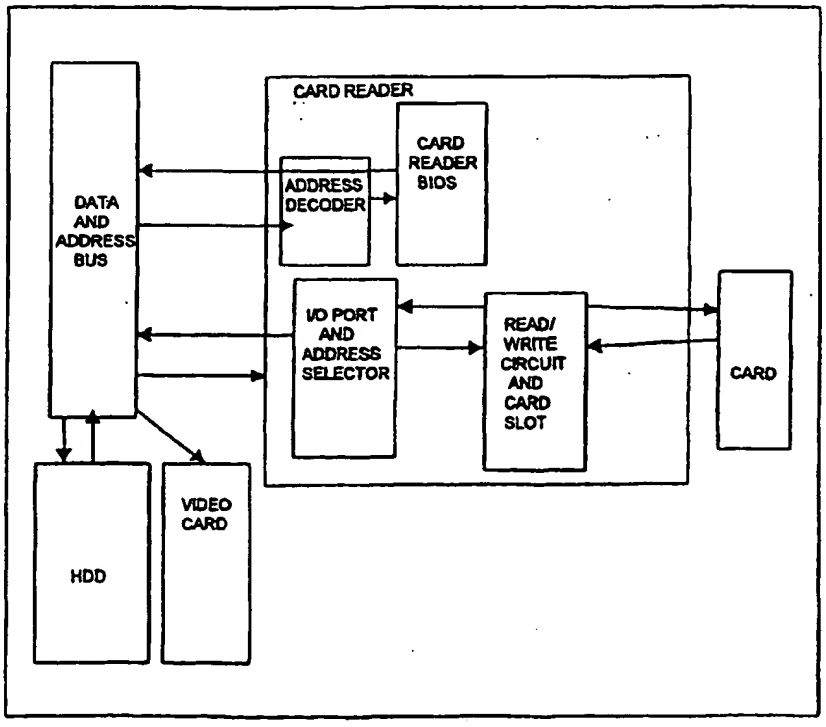
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND DEVICE OF DISABLING THE UNAUTHORISED USE OF A COMPUTER

(57) Abstract

The present invention relates to a method for avoiding unauthorised use of a personal computer by means of chip card and a respective installation. The booting of main processor unit is possible after entering of ID code stored on the chip card, during the power on self–test only. The chip card reader can be placed in 3.5'' floppy drive slot.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

METHOD AND DEVICE OF DISABLING THE UNAUTHORISED USE OF A COMPUTER

Field of the invention

This invention concerns a method of disabling the unauthorised usage of an IBM-compatible personal computer and/or data contained therein, using a chip card and chip card reader. It is also possible to integrate the hardware, required by the chip card reader, onto the motherboard of a computer. The invention disables the access to computer or data without a valid chip card. The invention includes a chip card, card ID, decrypting key, contained on the chip card, chip card reader, ISA bus add-on card for reader, reader BIOS (with address decoder and I/O ports) and chip card read/write electronics. There are different software solutions for keeping the decrypting key on the chip card and encrypting/decrypting algorithms in the card reader ROM. Also, in different solutions, the chip cards can be selected by type as required, i.e. the method and the reader are universal. The present invention is useful in the working places, where there are many people around and there is a danger of leaking confidential or secret data. However the use of the present invention is not restricted to this solution and the invention is applicable for various applications.

Background of the invention

When using computers for data processing and storage, it is very important to keep this data safe from unauthorised access. The contemporary methods are used widely to prevent data from unauthorised access, but they do not give enough protection. For example, US patent No. 5 187 352, G06K 005/00, (W. Blair, S. J. Brooks, 16.02.1993) discloses computer security system, that provides for controlled access to single or multiple components of a computer system. The system includes a magnetic card reading and encoding device that reads component access and time allotment data from a magnetically encoded card. In the US patent No. 4 575 703, G06K 013/04, (Sony Corporation, 11.03.1986) a card and device are disclosed for reading the data from the card.

The passwords, used in the boot process of a computer are easy to steal, one only has to look over the shoulder while the password is entered and memorise it. Also, there are factory passwords (Bypass password), which is the same for all motherboards of the same producer. Other authorisation methods, based on the chip cards, are relaying heavily on the software, which is easy to delete from the hard drive disk and after reboot, the safeguard is not active. For example, US patent No. 4 757 533, H04L, 009/00, (Computer Security Corporation, 12.07.1988) discloses a security system for a personal computer, in which hardware and software are combined to provide a tamper-proof manner of protecting user-access and file-access. This system for restricting unauthorised access uses chip card reader, which will use the software to check for the card, it's ID number, decrypting key and password during boot process, before the computer passes control to user. This process is not interruptible by user. The control over the computer stays with the card reader. After finishing the boot process, it is possible to use different software solutions, based on the chip card.

Chip cards and all the components used for electronics block (ISA card) are common and will not be discussed here. Also, the internal functions of a PC and used terminology are common.

Summary of the invention

The object of the present invention is to strengthen the security of the computer, i.e. disabling the theft of the data and unauthorised usage of a computer. At the same time, it is possible to use the invention to disable the access only to certain data (files, catalogues, logical drives, programmes), to collect and record different types of data (customer data, financial data, customer's recontra data, personal data and/or decrypting keys) to different chip cards, to process the data without physically typing the data in. The object of the invention is achieved by using the method and device described in more detail below, according to the appended claims.

Brief description of the drawings

Fig. 1 is the block diagram of the device according to the present invention.

Detailed description of the invention

According to the present invention, the authorisation of the user must be accomplished before giving control to the operating system. The card must be inserted in the card reader before the end of a boot process; the computer will then read the ID code from the card and compares it with the ID code, recorded during installation of the card reader. If there is decrypting algorithm present in the card reader's ROM, the decrypting key, used to access encrypted data, will also be read from the card. If there is no card present in the reader during boot process, the boot process will not be finished and the control will not be transferred to any operating system or external device (like floppy drive), thanks to the feature of the card reader of the invention. The data protection, using the chip card and reader, can be achieved in many ways.

According to the fist embodiment of the invention the card reader is initialized, using the standard computer BIOS – POST ROM Scan subfunction (search for add-on card BIOS's). The card reader BIOS will be found by extension BIOS attribute – the first two bytes (55h and Aah) in BIOS, beginning from address 0000. The control over the computer will be transferred to the card reader, which will read the installing signature from the computer hard drive disk. If the signature is not present, the control will be given back to computer and the boot will continue normally. This solution will not control the boot process, but it enables data exchange between the card reader and the computer, using different pieces of software.

According to the second embodiment of the invention the card reader is initialized, using the standard computer BIOS – POST ROM Scan subfunction (search for add-on card BIOS's). The cardreader BIOS will be found by extension BIOS attribute – the first two bytes (55h and Aah) in BIOS, beginning from address 0000. The control over the computer will be transferred to the card reader, which will read the installing signature from the computer's hard drive disk. If the signature is present, the chip card will be initialized by the command, protocol of which differs between different card

types. Then the ID code recorded in the card memory (offset 0) will be read and compared to the ID code on the hard drive disk. If the ID codes match, the control will be transferred back to computer BIOS and the boot process continues. In this situation the boot process is controlled and the data exchange between the computer and chip card is possible, using different pieces of software.

According to the third embodiment of the invention the card reader is initialized, using the standard computer BIOS - POST ROM Scan subfunction (search for add-on card BIOS's). The cardreader BIOS will be found by extension BIOS attribute – the first two bytes (55h and Aah) in BIOS, beginning from address 0000. The control over the computer will be transferred to the card reader, which will read the installing signature from the card ROM. If the signature is present, the chip card will be initialized by the command, protocol of which differs between different card types. Then the ID code recorded in the card memory (offset 0) will be read and compared to the ID code on the hard drive disk. If the ID codes match, the control will be transferred back to computer BIOS and the boot process continues. In this situation the boot process is controlled and the data exchange between the computer and chip card is possible, using different pieces of software.

All these instances have in common the possibility to control the computer's hardware clock's interrupt int. 1ch by software - this is achieved by storing the contents of a card reader BIOS in the computer memory as a TSR program, which controls the operation of the computer.

It is clear, that all the possibilities of the chip card usage for strengthening the data securiy of a computer, can be mixed different applications as needed and add program solutions of OS control for different cards. This means, that one can use different types of cards and different ID numbers in the same computer. It is possible to use PIC (Programmable Integrated Circuit) card, to boot the computer, but some other user can access his/her data or logical drive through the OS, using SIM-card. There is no need to change the card reader in order to change the chip card type; it is enough to change the reader's software accordingly.

The exemplary embodiment of the invention is described, based on fig. 1. On the fig. 1 is the block diagram of the device according to the invention. The electronics block of the card reader on fig. 1 is installed in the ISA or PCI bus connector. The card reader

slot is a separate unit, which is attached to a free 3.5" floppy disk slot. The card reader and electronics block are connected via flat-cable and according connectors.

The electronics block has a bi-directional bus buffer for buffering the data bus. The bus buffer is connected to chip card read/write circuitry, which in turn is connected to card reader device, attached to 3.5" floppy disk slot. The ISA or PCI card address decoder inputs are built so, that only addresses C000 to e800 are selected. This address range is assigned to add-on card BIOS's. To avoid possible BIOS address conflicts, the address decoder has an option to change the cardreader BIOS address. During the boot process, the computer BIOS checks for add-on cards and finds the card reader. The card reader then assumes the control over the computer. The I/O port selector gives the possibility to select different I/O port address in the rage from 300h to 3e0. The I/O address selector is technically similar to BIOS address decoder. All the communications between the computer and the card reader will be accomplished at this address through the selected I/O port.

CLAIMS

1. Method of disabling the unauthorised access to computer, the method comprising: inserting a chip card into the card reader and reading of data, stored on the chip card by the computer, wherein the card must be inserted before the end of a boot process – i.e. the chip card and the ID code contained on the chip card are read before any other program takes over.

2. Method according to the claim 1, comprising the steps of:
- initializing of the card reader by POST subfunction ROM SCAN, built in the computer's internal BIOS,
- finding of the card reader BIOS by the first two bytes of an extension BIOS of a cardreader, which are 55h and Aah, beginning from address 0000,
- transferring of the control over the computer to the card reader, which then reads the installation signature from the computer's hard drive disk,
- in the absence of the signature, transferring the control back to computer BIOS and the boot process resumes normally.

3. Method according to the claim 1, further comprising the steps of:
- on finding the installation signature present on the hard drive disk, the chip card will be initialized, using the protocol, which is corresponding to current chip card; the ID code stored on the chip card memory (offset 0) is read and compared to the ID code stored on the hard drive disk,
- if both ID codes match, the control is transferred back to computer and the boot process will resume normally.

4. Method according to the claim 1, further comprising the steps of:
- transferring the control over the computer to the card reader, which will read the installing signature from the card ROM,
- on finding the installation signature present on the hard drive disk, the chip card will be initialized, using the protocol, which is corresponding to current chip card; the ID code

stored on the chip card memory (offset 0) is read and compared to the ID code stored on the hard drive disk,

- if both ID codes match, the control is transferred back to computer and the boot process will resume normally.

5. Method according to the claim 1, wherein the boot process can be controlled or not controlled and data can be exchanged between the chip card and the computer, using different software solutions.

6. Method according to any preceding claims, wherein it is possible to take software control of the computer hardware clock interrupt 1 ch by reading the card reader BIOS into the computer memory as a TSR (resident) program, which controls the computer.

7. Method according to any preceding claims, wherein the described steps can be combined or added to operating system program solutions for different card types.

8. Device of disabling the unauthorised access to computer, comprising:
card reader device, bi-directional data bus buffer, electronic circuitry for reading and writing chip cards, ISA or PCI bus connector, card reader BIOS, address decoder for selecting address range C000 to e800 and input/output port with address selector for address range 300h to 3e0.

9. Device according to the claim 8, characterized in that the card reader device can be mounted into the 3.5" floppy disk slot.

10. Device according to the claim 8, characterized in that the device is interchangeable between other IBM-compatible PC-s.

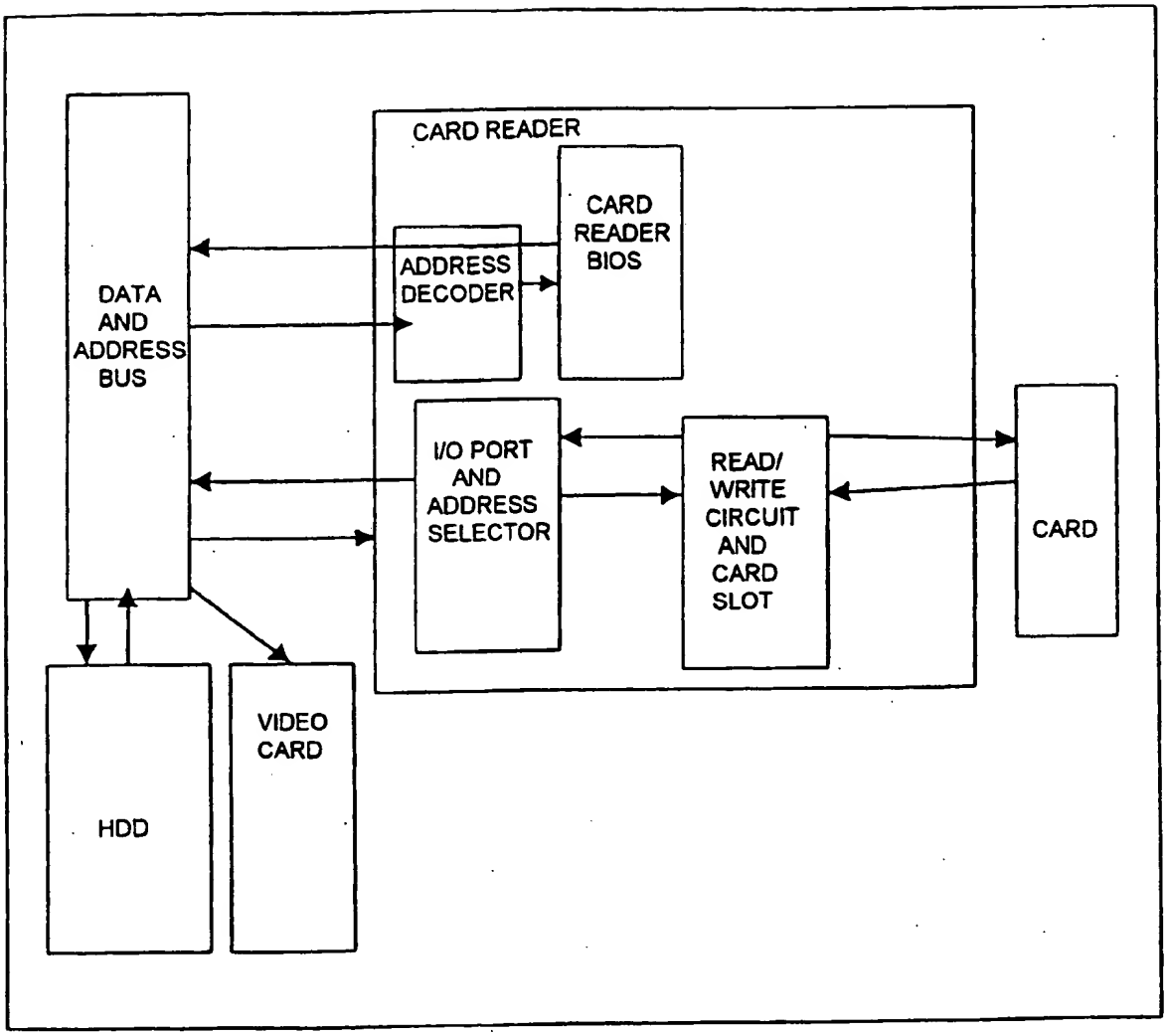

CARD READER
CARD READER BIOS
ADDRESS DECODER
DATA AND ADDRESS BUS
I/O PORT AND ADDRESS SELECTOR
READ/ WRITE CIRCUIT AND CARD SLOT
CARD
VIDEO CARD
HDD

FIG.1

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/EE 99/00001

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 610 981 A (MOONEY DAVID M ET AL) 11 March 1997 (1997-03-11) figures 1B-3,6,7A-7D column 4, line 45 -column 6, line 32 column 9, line 41 -column 10, line 13 column 12, line 44 -column 13, line 26	1-10
A	WO 97 16779 A (BUGOVICS JOZSEF ;ESD INFORMATION TECHNOLOGY ENT (DE)) 9 May 1997 (1997-05-09) figures 1,2 page 5, line 12 -page 7, line 2	1,3,4,8, 10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 December 1999	11/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Weiss, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr. ial Application No
PCT/EE 99/00001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5610981 A	11-03-1997	US 5327497 A	05-07-1994
		AT 175505 T	15-01-1999
		AU 703856 B	01-04-1999
		AU 2092695 A	25-09-1995
		BR 9506968 A	01-06-1999
		CA 2183759 A	14-09-1995
		CN 1146813 A	02-04-1997
		DE 69507129 D	18-02-1999
		DE 69507129 T	05-08-1999
		EP 0748474 A	18-12-1996
		NZ 282954 A	24-11-1997
		WO 9524696 A	14-09-1995
		AU 681588 B	04-09-1997
		AU 4528293 A	30-12-1993
		CA 2137274 A	09-12-1993
		EP 0643858 A	22-03-1995
		JP 7508604 T	21-09-1995
		WO 9324906 A	09-12-1993
		US 5515440 A	07-05-1996
WO 9716779 A	09-05-1997	DE 19540973 A	07-05-1997
		DE 29517410 U	18-01-1996